(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
1 juillet 2004 (01.07.2004)

PCT

(10) Numéro de publication internationale
WO 2004/056114 A1

(51) Classification internationale des brevets[7] : H04N 7/173, 7/167

(21) Numéro de la demande internationale : PCT/FR2003/050158

(22) Date de dépôt international : 9 décembre 2003 (09.12.2003)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
02/15540 9 décembre 2002 (09.12.2002) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **MEDIALIVE** [FR/FR]; 111, avenue Victor Hugo, F-75116 Paris (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **LECOMTE, Daniel** [FR/FR]; 157, rue de la Pompe, F-75116 Paris (FR). **GEORGES, Sébastien** [FR/FR]; 21, rue des Boulangers, F-75005 Paris (FR).

(74) Mandataire : **BREESE, Pierre**; BREESE-MAJEROWICZ, 3, avenue de l'Opéra, F-75001 Paris (FR).

(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) États désignés *(régional)* : brevet ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :
— *avec rapport de recherche internationale*
— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues*

[Suite sur la page suivante]

(54) Title: SYNCHRONISATION OF SECURE AUDIOVISUAL STREAMS

(54) Titre : SYNCHRONISATION DE FLUX AUDIOVISUELS SECURISES

(57) Abstract: The invention relates to a method for the synchronisation of video streams during the secure distribution of video sequences according to a nominal MPEG-type stream format, said sequences comprising a succession of images. According to the invention, before transmission to the client equipment, an analysis of the stream is performed in order to generate: (i) a modified main stream having the format of a nominal stream and comprising images which are modified through the substitution of certain data by data of the same type but random or calculated; and (ii) complementary information having any format and comprising the substituted data and the digital information which can be used to reconstruct the modified stream and which is referenced by synchronisation elements that can be used to ascertain to which image of the modified main stream they refer. Subsequently, the main stream is transmitted in real or delayed time and the complementary information is transmitted in real time, at the time of display, from the server towards the destination equipment. Next, a synthesis of a reconstructed stream with the nominal format is calculated on the destination equipment as a function of the main stream and the complementary information, and said reconstructed stream is read on the destination equipment. The sending of the complementary information is determined by reading the reconstructed stream, said information being sent in portions according to the position identifier transmitted by the destination equipment to the server.

(57) Abrégé : La présente invention concerne un procédé pour la synchronisation de flux vidéo lors de la distribution sécurisée de séquences vidéos selon un format de flux nominal de type MPEG constitués par une succession d'images. On procède, avant la transmission à l'équipement client, à une analyse du flux pour générer un flux principal modifié, présentant le format d'un flux nominal, et présentant des images modifiées par la substitution de certaines données par des données de même nature mais aléatoires ou calculées, et une information complémentaire d'un format quelconque, comportant les données substituées et les informations numériques aptes à permettre la reconstruction dudit flux modifié, référencées par des éléments de synchronisation permettant de savoir à quelle image du flux principal modifié elles se réfèrent, puis on transmet séparément, le flux principal en temps réel ou en temps différé et l'information complémentaire en temps réel au moment de la visualisation depuis le serveur vers l'équipement destinataire, et on calcule sur l'équipement destinataire une synthèse d'un flux reconstitué au format nominal en fonction dudit flux principal et de ladite information complémentaire et une lecture dudit flux reconstitué sur l'équipement destinataire. La lecture sur l'équipement destinataire conditionne l'envoi de ladite information complémentaire, celle-ci étant envoyée par portions en fonction dudit identifiant de position transmis par l'équipement destinataire au serveur.

WO 2004/056114 A1

SYNCHRONISATION DE FLUX AUDIOVISUELS SECURISES

La présente invention se rapporte au domaine du traitement de flux vidéo numériques.

On se propose dans la présente invention de fournir un système permettant de recomposer un contenu vidéo numérique préalablement embrouillé visuellement.

La présente invention se rapporte plus particulièrement à un dispositif capable de transmettre de façon sécurisée un ensemble de films de haute qualité visuelle vers un écran de visualisation type écran de télévision et/ou pour être enregistré sur le disque dur ou sur tout autre support d'enregistrement d'un boîtier reliant le réseau de télétransmission à l'écran de visualisation tel qu'un écran de télévision ou un moniteur d'ordinateur personnel, tout en préservant la qualité audiovisuelle mais en évitant toute utilisation frauduleuse comme la possibilité de faire des copies pirates de films ou de programmes audiovisuels enregistrés sur le disque dur ou tout autre support d'enregistrement du boîtier décodeur. L'invention concerne un système client - serveur et le mécanisme de synchronisation entre le serveur qui fournit le flux permettant le visionnage du film vidéo numérique sécurisé et le client qui lit et affiche le flux vidéo numérique.

Avec les solutions actuelles, il est possible de transmettre des films et des programmes audiovisuels sous forme numérique via des réseaux de diffusion de type hertzien, câble, satellite, etc. ou via des réseaux de télécommunication type DSL (Digital Subscriber Line) ou BLR (boucle locale radio) ou via des réseaux DAB (Digital Audio Broadcasting), etc. Par ailleurs, pour éviter le piratage

des œuvres ainsi diffusées, ces dernières sont souvent cryptées ou embrouillées par divers moyens bien connus de l'homme de l'art.

Toutefois, l'inconvénient principal de toutes les solutions actuelles (TiVo Inc., WO00165762) est qu'il faut transmettre non seulement les données cryptées vers les utilisateurs, mais également les clés de décryptage. La transmission des clés de décryptage pouvant se faire avant, en même temps ou après la transmission des programmes audiovisuels. Pour augmenter la sécurité et donc la protection des œuvres audiovisuelles contre une utilisation mal intentionnée, les clés de décryptage ainsi que les fonctions de décryptage des décodeurs audiovisuels peuvent comporter des moyens de sécurité améliorés comme des cartes à puces ou autres clés physiques qui peuvent en option, être mises à jour à distance.

Ainsi, les solutions actuelles appliquées à un boîtier décodeur avec possibilité d'enregistrement local de programmes audiovisuels sous forme numérique sur un support quelconque de type disque dur ou autre type de mémoire, offrent à un usager mal intentionné, la possibilité de faire des copies non autorisées des programmes ainsi enregistrés, puisqu'à un moment donné, cet usager possède avec son boîtier décodeur numérique, associé ou pas à des systèmes de cartes à puce, toutes les informations, programmes logiciels et données permettant le décryptage complet des programmes audiovisuels. En raison justement du fait qu'il possède toutes les données, l'usager mal intentionné aura la possibilité de faire des copies illégales sans que personne ne s'aperçoive de cette copie frauduleuse au moment où elle est faite.

Une solution consisterait donc à transmettre tout ou partie d'un programme audiovisuel numérique uniquement à la

demande (services de vidéo à la demande) à travers un réseau de télécommunication large bande de type ADSL, câble ou satellite, sans autoriser l'enregistrement local des programmes audiovisuels. Ici, l'inconvénient est tout autre et provient des performances de ces réseaux qui ne permettent pas de garantir des flux continus de quelques mégabits par seconde à chaque usager, comme exigé par les flux MPEG qui nécessitent des bandes passantes de quelques centaines de kilobits à plusieurs mégabits par seconde.

Dans ces conditions, une solution consiste à séparer le flux en deux parties dont aucune ne serait utilisable seule. Dans cette optique plusieurs brevets ont été déposés. Ainsi, on connaît par le document WO09908428 (Gilles Maton) un procédé de traitement multi-applicatif d'un terminal actif localisable dans lequel on réalise au moins une liaison avec un programme identifiable dédié à l'exécution d'une application, ledit programme dictant ses conditions d'exploitation au terminal pour la mise à disposition des fonctions. Le terminal dialogue ponctuellement, par l'emploi d'une liaison, avec le centre de gestion pour la réalisation, si nécessaire, des entrées et sorties des capacités de ce dernier, le centre de gestion devenant esclave ou non du terminal au niveau de l'applicatif vis-à-vis du programme entrant. Cette invention concerne également le procédé d'identification du programme et du terminal en exploitation. Ce procédé de l'art antérieur divise le flux en une partie servant à identifier l'utilisateur et une partie qui contient le programme à proprement parler. En particulier, ledit programme n'est pas inutilisable mais seulement verrouillé par la première partie. Enfin, ce brevet ne présente aucune solution pour synchroniser lesdites parties.

D'autre part, le document EP0778513 (Matsushita) décrit un procédé permettant de prévenir l'utilisation illégale d'une information en y ajoutant une information de contrôle afin de vérifier les droits de l'utilisateur. Le système permet de savoir en permanence quelle partie de l'information est utilisée et par quel utilisateur et par là de savoir si cet utilisateur est en position illégale ou pas. Ce procédé sécurise donc les données en y ajoutant des informations additionnelles qui dénaturent l'information initiale.

Le document WO0049483 (Netquartz) nous offre également des procédés et des systèmes pour créer un lien entre les utilisateurs et un éditeur d'entités numérisées. Le procédé comprend l'une au moins des étapes suivantes : l'étape de subdiviser ladite entité numérisée en deux parties ; l'étape de mémoriser une partie dans une zone mémoire d'un serveur connecté à un réseau informatique ; l'étape de transmettre l'autre partie à au moins un utilisateur disposant d'un équipement informatique ; l'étape de connecter ledit équipement informatique audit réseau informatique ; l'étape d'établir un lien fonctionnel entre ladite première partie et ladite deuxième partie. Ces procédés et systèmes ne spécifient pas d'une part si la partie mémorisée sur le serveur peut être stockée par l'utilisateur ce qui permettrait à celui-ci de pirater ladite entité numérisée, et d'autre part la façon de synchroniser lesdites deux parties.

Enfin, dans cette approche, l'état de la technique le plus proche se retrouve dans les brevets d'HyperLOCK Technologies dont le plus pertinent est le document US05937164. Cette invention utilise la solution qui consiste à séparer le flux en deux parties dont la plus petite détient une information nécessaire à l'utilisation de la

plus grande. Cependant, ce brevet n'est pas suffisant pour répondre au problème identifié. En effet, la suppression d'une partie du flux dénature le format du flux, et ne peut donc pas être reconnu comme un flux standard, exploitable avec des applications logicielles générales. Ce procédé de l'art antérieur nécessite à la fois un logiciel spécifique côté serveur, pour la séparation des deux parties, et un autre logiciel spécifique assurant non seulement la reconstruction du flux, mais également l'acquisition du flux principal et son exploitation selon un format propriétaire à la solution. Ce format propriétaire n'est pas le format initial du flux avant séparation en deux parties, dans cette solution connue.

Cette société a également déposé trois autres brevets : le document US5892825 reprend le brevet précédent mais dans un cadre moins large car les flux y sont toujours cryptés ; le document US6035329 repose sur le même principe, il concerne un procédé permettant la lecture d'un disque de type CD-ROM ou DVD-ROM conditionnellement à l'identification des droits par l'insertion d'une carte à puce sur laquelle les informations nécessaires à la lecture sont stockées. Ce procédé n'est encore pas suffisant pour notre problème car il ne garantit pas que le flux modifié soit du même format que le flux originel. Enfin, le document US6185306 concerne un procédé de transmission de données cryptées depuis un site Web vers un ordinateur demandeur. Ce procédé permet cependant à l'utilisateur de disposer à un moment donné de tous les outils nécessaires pour copier les données.

Une autre référence de l'art antérieur est le document WO 00/44172 qui présente un système de distribution de vidéo à la demande consistant à transmettre des flux vidéos cryptés depuis un fournisseur vers un ou plusieurs

récepteurs. La vidéo cryptée est stockée au préalable chez le récepteur et est visualisée ultérieurement. La requête de visualisation est adressée à un émetteur vidéo qui envoie l'information de décryptage pour une visualisation immédiate du flux vidéo. L'information de décryptage est envoyée au récepteur par voie séparée ou par la même voie que la vidéo cryptée. Avant l'envoi des clés (statiques ou dynamiques) pour le décryptage, est effectuée une étape d'identification du récepteur. Cet art antérieur décrit donc un système de cryptage à l'aide de clé(s) bien connu par l'homme de l'art. Toutefois, la totalité du flux vidéo protégé par cryptage est stockée chez le récepteur, l'ensemble des données du flux vidéo se trouve à l'intérieur de la vidéo protégée, il peut donc être vulnérable au piratage.

L'art antérieur connaît également le document US 2002/0164024 A1 qui concerne un système de traitement de données vidéos et audio basé sur une relation de prédiction entre trames, contenant un module de fragmentation des données, un module de cryptage d'une partie des données, un module d'envoi, un module pour différencier le traitement par type de trames I, P, B et leur rangement dans des files séparées, un module de réception, un module de décryptage et un module d'assemblage des données. Le processus de cryptage est effectué uniquement sur des fragments comportant des images I, qui sont décryptées et re-assemblées dans le récepteur, reconstituant ainsi la vidéo, la reconstitution étant effectuée en alignant les paquets par ordre croissant de la référence de temps indiquée dans le flux binaire. Ce document décrit un système de cryptage « classique », avec optimisation du cryptage. La fragmentation est appliquée dans le but de séparer les images I du reste du flux afin de les crypter. Après ce cryptage sélectif, les fragments sont

envoyés en utilisant différentes files d'attente. Cependant, toutes les données du flux audiovisuel restent à l'intérieur du flux protégé, tout ou partie du flux étant pas crypté.

Enfin, le brevet WO 01/97520 présente également des méthodes, des procédés et des dispositifs pour contrôler la transmission et l'enregistrement des contenus numérisés de type MPEG-2. Toutefois, ce brevet ne présente aucune spécificité pour la synchronisation des flux qui constituent les deux parties d'un même programme audiovisuel. De plus, la méthode décrite dans ce brevet est totalement inefficace pour les réseaux de télécommunication bas débit, car elle substitue tout ou partie des images I dont le poids en octets est très coûteux lors de la transmission du deuxième flux.

Afin de corriger ces différents défauts, l'invention concerne dans son acceptation la plus générale un procédé pour la distribution de séquences vidéos selon un format de flux nominal constitué par une succession d'images, ledit flux sur lequel on procède, avant la transmission à l'équipement client, à une analyse pour générer un flux principal modifié, présentant le format du flux nominal, et présentant des images modifiées par la substitution de certaines données par des données de même nature mais aléatoires ou calculées, et une information complémentaire d'un format quelconque, comportant les données substituées et les informations numériques aptes à permettre la reconstruction dudit flux nominal modifié, puis à transmettre séparément, le flux principal modifié en temps réel ou en temps différé et l'information complémentaire en temps réel au moment de la visualisation depuis le serveur vers l'équipement destinataire, et pour lequel on calcule sur l'équipement destinataire une synthèse d'un flux

disponible au format nominal, reconstitué en fonction dudit flux principal modifié et de ladite information complémentaire et une lecture dudit flux disponible sur l'équipement destinataire caractérisé en ce que ledit procédé comporte, pendant ladite lecture dudit flux, une étape consistant à générer un identifiant de position en fonction d'une caractéristique dudit flux lu, cet identifiant de position étant transmis au serveur activant en réponse l'envoi de l'information complémentaire fonction dudit identifiant de position.

Selon une première variante, chaque image du flux nominal est associée à un indicateur de position.

Selon une deuxième variante, l'étape de lecture comporte une opération de calcul de l'identifiant de position de l'image lue.

Selon une troisième variante, l'étape de lecture comporte une opération de calcul de l'identifiant de position du flux lu.

Avantageusement, l'information complémentaire est envoyée par portions.

Selon un mode de réalisation particulier de l'invention, le flux disponible sur l'équipement destinataire dont la lecture conditionne la position et la portion à envoyer de ladite information complémentaire est une partie du flux principal modifié.

Selon un autre mode de réalisation, le flux disponible sur l'équipement destinataire dont la lecture conditionne la position et la portion à envoyer de ladite information complémentaire est une partie du flux nominal reconstitué.

Dans un mode de mise en œuvre particulier de l'invention, le format de flux nominal est défini par la norme MPEG-2. Dans ce cas particulier de réalisation, ledit identifiant de position pour une image est constitué des

variables "time_code", ou code temporel, associé au groupe d'images dans lequel se trouve l'image considérée et "temporal_reference", ou référence temporelle, pour l'image, qui sont des variables définies par MPEG-2.

Avantageusement, chaque portion de ladite information complémentaire envoyée par le serveur permet de reconstituer au moins une image du flux originel lors de ladite synthèse.

Selon un mode de mise en œuvre particulier, le serveur adapte la taille et le contenu de chaque portion de ladite information complémentaire à envoyer en fonction dudit identifiant de position.

Dans un mode de réalisation préféré, chaque portion de ladite information complémentaire est envoyée en avance par rapport à l'instant d'affichage de ladite image du flux reconstituée avec ladite portion.

Dans un mode de mise en œuvre, le serveur adapte l'envoi d'information complémentaire, lorsque l'utilisateur de l'équipement destinataire fait « pause », en arrêtant l'envoi de l'information complémentaire. De même, le serveur adapte l'envoi d'information complémentaire, lorsque l'utilisateur de l'équipement destinataire fait « avance rapide » ou « retour rapide », en envoyant la portion correspondant à la position adéquate pour les commandes « avance rapide » et « retour rapide ». De la même façon, le serveur adapte l'envoi d'information complémentaire lorsqu'une panne réseau survient qui empêche la communication client - serveur, en arrêtant l'envoi d'information complémentaire durant la panne et en le reprenant lorsque la panne cesse et qu'il reçoit de nouveau les messages en provenance du client.

Avantageusement, le serveur crée, préalablement à l'envoi de l'information complémentaire, un tableau associant des pointeurs vers des portions de l'information

complémentaire avec des positions temporelles relatives à des images du flux vidéo, stocke ledit tableau sur un support relié au serveur et consulte ledit tableau pour déterminer la portion d'information complémentaire à envoyer après avoir reçu ledit identifiant de position.

L'invention concerne également un équipement pour la fabrication d'un flux vidéo en vue de la mise en œuvre du procédé tel que décrit ci-dessus, comportant au moins un serveur multimédia contenant les séquences vidéos originelles, un dispositif d'analyse du flux vidéo provenant dudit serveur pour générer ledit flux principal modifié et ladite information complémentaire et qui comprend en particulier un dispositif de synchronisation de l'envoi de ladite information complémentaire en fonction dudit identifiant de position envoyé par l'équipement destinataire.

L'invention concerne enfin un système pour la transmission d'un flux vidéo selon le procédé décrit ci-dessus, comprenant un équipement de production d'un flux vidéo, au moins un équipement d'exploitation d'un flux vidéo et au moins un réseau de communication entre l'équipement de production et le(s) équipement(s) d'exploitation.

La présente invention sera mieux comprise à la lecture de la description d'un exemple non limitatif de réalisation qui suit, se référant aux dessins annexés où :

- la figure 1 décrit l'architecture d'ensemble d'un système pour la mise en œuvre du procédé selon l'invention ;

- la figure 2 représente un mode de réalisation particulier du système de synchronisation des flux audiovisuels conforme à l'invention.

Le principe général d'un procédé de sécurisation d'un flux vidéo est exposé ci-après. L'invention concerne un

procédé pour la distribution de séquences vidéos numériques selon un format de flux nominal constitué par une succession d'images (« pictures » en anglais ou pour le format MPEG) comprenant chacune au moins un bloc numérique regroupant un certain nombre de coefficients correspondant à des éléments vidéo simples codés numériquement selon un mode précisé à l'intérieur du flux concerné et utilisé par tous les décodeurs vidéos capables de l'afficher afin de pouvoir la décoder correctement et éventuellement organisées de façon hiérarchique en groupe d'images et séquences.

Avantageusement le format contient un moyen de localisation de ladite image numérique dans le flux à l'aide d'un identifiant de position temporelle permettant de savoir à quel moment l'image en question doit être affichée.

Ce procédé comporte :

- une étape préparatoire consistant à modifier au moins un desdits éléments d'une desdites images, le flux binaire ainsi généré étant appelé flux principal modifié ;
- une étape de transmission :
  - o du flux principal modifié conforme au format du flux nominal, constitué par des images contenant les éléments modifiés au cours de l'étape préparatoire et
  - o d'une information numérique complémentaire par une voie séparée dudit flux principal modifié, permettant de reconstituer le flux originel à partir du calcul, sur l'équipement destinataire, en fonction dudit flux principal modifié et de ladite information complémentaire. On définit ladite information complémentaire comme un ensemble constitué de données (par exemple des éléments décrivant le flux numérique originel ou extraits du flux originel) et de fonctions (par exemple, la fonction substitution ou permutation). Une fonction est définie comme contenant au moins une instruction mettant en rapport des

données et des opérateurs. Ladite information complémentaire décrit les opérations à effectuer pour récupérer le flux originel à partir du flux principal modifié.

La reconstitution du flux originel s'effectue sur l'équipement destinataire à partir du flux principal modifié déjà présent sur l'équipement destinataire ou envoyé en temps réel et de l'information complémentaire envoyée en temps réel au moment de la visualisation comprenant des données et des fonctions exécutées à l'aide de routines (ensemble d'instructions) numériques. L'information complémentaire est envoyée par le serveur en fonction de la position de la tête de lecture dans le flux disponible sur l'équipement client. Cette position, définie par un identifiant de position ou élément de synchronisation, est envoyée régulièrement par le client au serveur suivant l'instant de visionnage par le client du flux disponible sur l'équipement client. Ledit flux disponible sur l'équipement client est identique au flux originel si le client possède les droits pour l'afficher et s'il est en connexion avec le serveur contenant l'information complémentaire, ou identique au flux principal modifié si ce n'est pas le cas.

Quand le flux disponible sur l'équipement destinataire est identique au flux originel, l'utilisateur peut le visionner sur son écran et si l'utilisateur désire se déplacer dans la séquence vidéo, le client informe le serveur de la nouvelle position de la tête de lecture et le serveur envoie alors l'information complémentaire nécessaire au client pour reconstituer la portion du film qu'il regarde désormais.

Dans la présente invention, on entend sous le terme « embrouillage » la modification d'un flux vidéo numérique par des méthodes appropriées de manière à ce que ce flux reste conforme à la norme avec laquelle il a été encodé

numériquement, tout en le rendant jouable par un afficheur vidéo, mais altéré du point de vue de la perception visuelle humaine.

Dans la présente invention, on entend sous le terme « désembrouillage » le processus de restitution par des méthodes appropriées du flux initial, le flux vidéo restitué après le désembrouillage étant identique au flux vidéo initial.

La présente invention propose une protection grâce à un embrouillage du flux vidéo fondée intégralement sur sa structure, protection qui consiste à modifier des parties ciblées du « bitstream » (flux binaire structuré) essentielles pour la compréhension du film par un œil humain. Les vraies valeurs de ces parties ciblées sont extraites du bitstream et stockées en tant qu'information complémentaire, et à leurs places sont mises des valeurs aléatoires ou calculées ou des valeurs permutées, et cela sur la totalité du flux vidéo. Ainsi, on rajoute des « leurres » pour le décodeur, c'est-à-dire des valeurs compréhensibles pour le décodeur, mais non identiques à celles présentes dans le flux nominal, qui reçoit en entrée un flux vidéo complètement conforme au format vidéo d'origine, mais qui n'est pas acceptable du point de vue perception visuelle par un être humain.

A l'inverse de la plupart des systèmes de cryptage déjà connus par l'homme de l'art, le principe décrit ci-dessous permet d'assurer un haut niveau de protection sans nécessiter une liaison client - serveur haut débit puisque ladite information complémentaire à envoyer ne représente qu'un faible pourcentage du flux vidéo d'origine, le flux principal modifié étant déjà présent sur l'équipement du client.

La protection, réalisée de façon conforme à l'invention, est basée sur le principe de la suppression et/ou du remplacement d'informations décrivant le signal vidéo par une méthode quelconque, soit : substitution, modification ou déplacement de l'information. Cette protection est également basée sur la connaissance de la structure du flux à la sortie de l'encodeur vidéo : l'embrouillage dépend du contenu dudit flux vidéo numérique. La reconstitution du flux originel s'effectue sur l'équipement destinataire à partir du flux principal modifié déjà présent ou reçu en temps réel sur l'équipement destinataire et de l'information complémentaire envoyée en temps réel au moment de la visualisation comprenant des données et des fonctions exécutées à l'aide de routines (ensemble d'instructions) numériques.

La présente invention concerne en particulier le processus de synchronisation entre le fournisseur de l'information complémentaire (le serveur) et le lecteur/afficheur installé chez le client. Pour cela l'invention utilise des éléments de synchronisation (ou identifiants de position de la tête de lecture dans le flux disponible sur l'équipement destinataire) qui permettent de faire le lien entre une portion donnée de l'information complémentaire et la partie du flux principal modifié qu'elle permet de modifier afin de reconstituer la partie correspondante du flux nominal. Par exemple l'invention utilise des données de position temporelle relatives à la tête de lecture du client dans le flux vidéo disponible sur l'équipement client, comme celles contenues dans un flux MPEG, pour déterminer l'information complémentaire à envoyer.

Une autre possibilité, correspondant à un autre exemple de réalisation, est de numéroter les images du flux

principal modifié et d'indiquer, dans les différentes portions de l'information complémentaire, le numéro de l'image ou des images du flux principal modifié que ladite portion permet de modifier afin de reconstituer la partie correspondante du flux nominal.

Un autre exemple de réalisation consiste à utiliser des mots binaires calculés à partir du flux principal modifié, un mot binaire donné étant spécifique à une portion du flux principal modifié donnée, qui est alors spécifié dans la portion de l'information complémentaire correspondante.

Un autre exemple de réalisation consiste à utiliser des mots binaires calculés à partir du flux principal modifié, un mot binaire donné étant spécifique à une image du flux principal modifié donnée, qui est alors spécifié dans la portion de l'information complémentaire correspondante.

Un autre exemple de réalisation consiste à ajouter un mot binaire unique dans chaque champ utilisateur du flux principal modifié (champ « user data » de MPEG-2 par exemple), et dans la portion de l'information complémentaire correspondante. Un champ utilisateur est caractérisé en ce qu'on peut y ajouter des informations binaires sans que cela n'affecte l'affichage du flux binaire vidéo le contenant.

Quelle que soit la solution choisie, le client envoie régulièrement au serveur l'identifiant de position de la tête de lecture du client dans le flux disponible sur l'équipement destinataire (position temporelle ou mot binaire) permettant au serveur de déterminer la portion de l'information complémentaire dont l'équipement client a besoin pour transformer le flux principal modifié afin de reconstituer la partie correspondante du flux nominal.

L'invention sera mieux comprise à la lecture d'un exemple de réalisation de l'invention, en se référant aux figures 1 et 2.

Dans cet exemple de réalisation, l'invention concerne une séquence vidéo encodée selon le format MPEG-2, sans que cela constitue une réduction de la portée de la présente invention.

Sur la figure 1, l'agencement d'interfaçage vidéo (8) est adapté pour relier au moins un dispositif d'affichage, par exemple un moniteur, un vidéo projecteur ou un dispositif de type écran de télévision (6), à au moins une interface de réseau de transmission et de diffusion large bande (4) et à au moins une interface de réseau de télécommunication (10). Selon la présente invention, cet agencement est composé d'un module (8) comprenant principalement, d'une part, une unité de traitement adaptée pour traiter, en particulier décoder et désembrouiller tout flux vidéo de type MPEG-2 selon un programme logiciel de décodage et désembrouillage pré-chargé, de manière à l'afficher, en temps réel ou différé, de le stocker, de l'enregistrer et/ou de l'envoyer via un réseau de télécommunication et, d'autre part, au moins une interface d'écran (7) et une interface de connexion à un réseau local ou étendu (5) et/ou (9). Le réseau de transmission et de diffusion large bande (4) et le réseau de télécommunication (10) pouvant être confondus en un seul réseau.

Le disque dur ou le dispositif d'enregistrement du module (8) peut être utilisé comme mémoire tampon pour stocker momentanément au moins une partie du programme ou de la séquence vidéo à afficher, en cas de visualisation différée ou de limitation dans la bande passante du réseau de transmission. La visualisation peut être retardée ou différée à la demande de l'utilisateur ou du portail (12).

Comme le montre la figure 1, l'interface de connexion (5) est reliée à un réseau de transmission et de diffusion large bande (4) telle qu'un modem, un modem satellite, un modem câblé, d'une interface de ligne à fibre optique ou d'une interface radio ou infrarouge pour la communication sans-fil.

C'est par cette liaison classique de diffusion vidéo que seront transmis les contenus des programmes audiovisuels comme des films. Toutefois, de façon à ne pas laisser faire de copies pirates, avant de transmettre le contenu audiovisuel depuis le serveur (1) ou le portail (12) il est prévu de conserver une petite partie du contenu audiovisuel dans le portail (12).

En cas de visualisation d'un programme audiovisuel en temps réel, cette petite partie du contenu audiovisuel conservée dans le portail (12) sera également envoyée au module (8) en temps réel, via le réseau de télécommunication (10).

Dans le format MPEG-2, le flux audiovisuel est divisé en une hiérarchie de structures imbriquées les unes dans les autres. Ainsi, un « flux » contient un nombre indéfini de groupes d'images liées les unes aux autres (« GOP » : « Group of Pictures ») ; un groupe d'images contient un certain nombre d'images (généralement 12 ou 15 pour MPEG mais ce n'est pas obligatoire) ; une image est décomposée en tranches (« slices ») ; une tranche contient une série de macroblocs ; un macrobloc regroupe entre 6 et 12 blocs ; un bloc contient l'information relative à un carré de 8 pixels sur 8 sous formes de coefficients fréquentiels. Le flux est compressé par une transformation à cosinus discret (DCT), qui s'applique sur chaque bloc de façon à concentrer l'information pertinente dans seulement certains coefficients de façon à pouvoir supprimer les autres et

ainsi réduire la quantité d'information à stocker, et à un échantillonnage des coefficients transformés et un codage destiné à réduire la taille du flux (par exemple un codage à longueur variable ou un codage de type « Run-Level »).

Dans cet exemple de réalisation, décrit en référence aux figures 1 et 2, le flux nominal (101) provient du serveur (1) pour être transmis au portail (12). Le dispositif d'analyse (121) du portail (12) procède à l'analyse du flux nominal (101) pour constituer d'une part le flux principal modifié (122) et d'autre part l'information complémentaire (123). Le flux principal modifié (122) est transmis au client d'une manière quelconque. Cette manière peut être : à travers un réseau large bande (4) de type BLR ou DSL, à travers un réseau mobile de type GSM, ou encore grâce à un CD-ROM ou un autre support physique. Le client stocke le flux principal modifié (122) sur un support physique (85) situé chez lui, ledit support physique pouvant être un disque dur ou un CD-ROM.

Lorsque le client (8) désire regarder la séquence vidéo correspondant à ce flux principal modifié, il adresse la demande au serveur (12), en spécifiant un identifiant de la séquence vidéo demandée et en fournissant au moins un identifiant du client (8). Le serveur (12) reçoit la demande du client et vérifie si celui-ci a le droit de regarder la séquence demandée, en utilisant l'identifiant de la séquence et celui du client. Cette vérification peut être faite par exemple à l'aide d'une base de données répertoriant pour chaque client la liste des séquences vidéo autorisées.

Si le client (8) est autorisé à regarder la séquence vidéo demandée, le serveur (12) établit une connexion avec le client pour transmettre l'information complémentaire (123) à travers le réseau (10). Lorsque la connexion est établie, le client (8) envoie au serveur (12) les

identifiants de position de la tête de lecture dans le flux vidéo demandé. Le serveur (12) reçoit les informations de position et adapte le contenu de l'information complémentaire (123) transmise au client à travers la liaison (10) en fonction de ladite position.

Dans une autre réalisation de cette invention, les informations de position sont transmises en même temps que la demande pour la séquence vidéo et le serveur commence la diffusion de l'information complémentaire correspondant à ladite position après avoir vérifier l'autorisation.

Le client (8) reçoit la partie de l'information complémentaire (123) correspondant à la position de la tête de lecture et la stocke dans le tampon d'entrée (86). Ce tampon est de préférence une mémoire volatile. Dans le même temps, le client lit à partir du support de stockage (85) le flux principal modifié correspondant à cette position via le tampon de lecture (83). Le dispositif de synthèse (87) utilise l'information complémentaire stockée dans le tampon d'entrée (86) et le flux principal stocké dans le tampon de lecture (83) pour reconstituer sans erreur le flux originel et l'envoyer vers le lecteur (81). Le flux originel, lu par le lecteur (81), est alors affiché sur le dispositif d'affichage (6).

Dans cet exemple de réalisation, deux variables pour chaque image du flux sont utilisées comme identifiant de position : la variable « temporal_reference » ou référence temporelle, présente dans le champ « picture_header » ou en-tête d'image pour chaque image, et la variable « time_code » ou code temporel, présente dans le champ « Group Of Pictures Header » ou en-tête de groupe d'images pour le groupe d'images dans lequel se trouve l'image considérée. Ces variables permettent d'identifier de manière unique une image dans un flux vidéo MPEG-2 d'une durée totale

inférieure à 24h. Le client envoie régulièrement au serveur sa position dans le flux vidéo en lui communiquant ces deux données. Le serveur adapte la portion de l'information complémentaire à envoyer en fonction de cette position. Chaque portion de l'information complémentaire contient en effet une copie de ces identifiants de position ou éléments de synchronisation permettant de faire un lien unique entre l'image du flux principal modifié et la portion de l'information complémentaire correspondante qui permet de modifier le flux principal modifié afin de reconstituer la partie correspondante du flux nominal. Dans cet exemple de réalisation, l'information complémentaire est contenue dans un fichier unique. Lorsque le serveur (12) reçoit les variables de position provenant du client, il détermine la portion de l'information complémentaire à envoyer en parcourant ledit fichier. Pour que la recherche de la portion voulue soit plus rapide, l'invention peut avantageusement utiliser un tableau qui fait correspondre une position dans ledit fichier avec une image du flux principal embrouillé, ce tableau étant réalisé lors d'une phase préalable, associée à l'analyse du flux principal.

Dans un mode de réalisation alternatif, l'élément de synchronisation ou identifiant de position de la tête de lecture dans le flux disponible sur l'équipement destinataire est le numéro de l'image courante, c'est-à-dire l'ordre d'apparition de ladite image au sein du flux principal modifié correspondant. Par exemple, la première image du flux principal modifié aura le numéro 1, la deuxième le numéro 2, et la 22ème le numéro 22. Ce numéro est également indiqué dans l'information complémentaire de façon à être capable de faire le lien entre l'image du flux principal modifié et la portion de l'information complémentaire correspondante qui permet de transformer le

flux principal modifié afin de reconstituer la partie correspondante du flux nominal.

Dans un troisième exemple de réalisation, les éléments de synchronisation ou identifiants de position de la tête de lecture dans le flux disponible sur l'équipement destinataire sont des mots binaires calculés à partir du flux principal modifié, un mot binaire donné étant spécifique au contenu d'une portion donnée du flux principal modifié, ladite portion étant caractérisée par sa position binaire, définie par le nombre de bits qui la séparent du début du flux, et sa taille, ledit mot binaire étant spécifié dans la portion de l'information complémentaire correspondante. Ce mot binaire est calculé d'après le contenu binaire de ladite portion de façon à ce que deux portions référencées différentes produisent des mots binaires différents. Pour obtenir le mot binaire, on peut utiliser une table de « hash » code. Une table de « hash » code est un ensemble d'entrées, où chaque entrée est constituée d'une clé et d'une valeur. On ne peut avoir deux entrées ayant la même clé. A partir d'une clé, une table de « hash » code peut retrouver très rapidement l'entrée correspondante. Il existe de nombreux algorithmes de ce genre qui sont notamment utilisés dans les télécommunications pour détecter les erreurs de transmission.

Dans une variante de réalisation de l'exemple précédent, ledit mot binaire n'est pas calculé d'après le contenu binaire d'une portion du flux principal modifié caractérisée par sa position binaire et sa taille, mais d'après le contenu binaire d'une image du flux principal modifié donnée.

Dans un autre exemple de réalisation, les éléments de synchronisation ou identifiants de position de la tête de

lecture dans le flux disponible sur l'équipement destinataire sont des mots binaires insérés dans chaque champ utilisateur du flux principal modifié (champ « user data » de MPEG-2 que l'on peut insérer avant chaque image d'un flux vidéo MPEG-2), et dans la portion de l'information complémentaire correspondante. Chaque mot binaire est différent de façon à ce que le lien entre une image du flux principal modifié et une portion de l'information complémentaire soit unique.

Quel que soit le mode de constitution desdits identifiants de position de la tête de lecture, en fonctionnement normal et continu d'affichage du flux vidéo (lecture simple), le client (8) envoie au serveur une information de position correspondant à la dernière image ou à la dernière portion affichée du flux disponible sur l'équipement destinataire qui peut être soit issue du flux principal modifié si le client n'a pas reçu l'information complémentaire correspondante pour modifier le flux principal modifié afin de reconstituer la partie correspondante du flux nominal, soit issue du flux reconstitué identique au flux nominal dans le cas contraire. Le serveur reçoit cette information de position et calcule la portion d'information complémentaire à envoyer pour permettre le visionnage du contenu suivant cette dernière position affichée. Dans l'exemple de réalisation qui nous intéresse, ce calcul est possible grâce à la correspondance entre les couples référence temporelle (code temporel présent dans les messages envoyés par le client vers le serveur) et les couples de même nature inscrits dans l'information complémentaire. En fonctionnement normal, la position envoyée par le client (8) correspond à une portion d'information complémentaire récemment envoyée par le

serveur (12). Celui-ci envoie donc la portion suivante de l'information complémentaire au client (8) par le réseau (10). Cette portion correspond en fait à des images que le client va bientôt afficher sur le dispositif d'affichage (6), pour laisser le temps au dispositif de synthèse (87) de désembrouiller le flux. Si le serveur envoyait l'information complémentaire correspondant à ce que le client est en train d'afficher, celle-ci arriverait trop tard chez le client pour pouvoir être utilisée, il faut donc l'envoyer avec une légère anticipation. Le serveur (12) envoie l'information complémentaire par paquets, chaque paquet comprenant l'information nécessaire pour reconstituer plusieurs images. Si chaque paquet correspond à une durée t de la séquence vidéo et que la transmission du paquet occupe une durée t', le serveur (12) attend une durée $(t-t')$ entre la fin de la transmission d'un paquet et le début de la transmission du paquet suivant. A la fin de cette attente, le serveur se réveille et analyse les messages en provenance du client. Ces messages conditionnent alors le comportement du serveur de la façon décrite ci-dessus.

Le serveur (12) envoie des portions d'information complémentaire tant qu'il reçoit des messages du client (8) lui donnant la position de la tête de lecture. Lorsque le client arrête la lecture (« pause » ou « stop » ou déconnexion réseau), il arrête d'envoyer des informations de position au serveur. Dans cet exemple réalisé, si le serveur ne reçoit pas de messages de l'équipement client pendant le temps nécessaire à celui-ci pour visionner le flux vidéo correspondant au dernier paquet d'information complémentaire envoyé (durée t), c'est-à-dire s'il n'a pas reçu de nouveaux messages lors de son réveil, il arrête d'envoyer des portions d'information complémentaire.

L'envoi de portions d'information complémentaire reprend quand le client recommence à lire la séquence vidéo et donc à envoyer des informations de position. Ainsi, dans le cas d'une panne de réseau empêchant la communication entre l'équipement client et le serveur, lorsque la panne survient, le serveur cesse de recevoir des identifiants de position de la tête de lecture et stoppe donc l'envoi de l'information complémentaire ; et lorsque la panne cesse, l'équipement client envoie sa position courante dans le flux disponible sur l'équipement client, le serveur la reçoit, s'y adapte et envoie l'information complémentaire correspondante. De même dans le cas d'une « pause » ou d'un arrêt du visionnage du flux vidéo par le client, le serveur ne reçoit plus de messages du client et stoppe donc l'envoi de l'information complémentaire : celui-ci reprend lorsque le client reprend la lecture du flux vidéo disponible sur l'équipement client.

Avantageusement, dans le cas où le client souhaite arrêter de regarder le flux vidéo pour une durée prolongée, la session client - serveur est fermée. Lorsque la session reprend suite à la volonté du client de reprendre le visionnage du flux vidéo et à sa reconnexion au serveur, le serveur envoie l'information complémentaire à partir de la portion correspondant à celle qu'il recevait avant la fin de session. L'affichage du flux vidéo sur l'équipement client ne reprend qu'au moment où il commence à recevoir les informations complémentaires de la part du serveur.

Si le client fait un retour en arrière dans la séquence vidéo, la nouvelle position envoyée au serveur est une position antérieure à la dernière position envoyée. L'envoi suivant du serveur est donc une partie de l'information complémentaire située avant la dernière partie envoyée. La quantité et donc la durée de l'information

complémentaire envoyée par le serveur dépend de la vitesse arrière qui a été choisie par le client. Cette fonctionnalité permet d'offrir plusieurs vitesses de retour arrière sur l'équipement du client.

De même, si le client envoie une commande « avance rapide » dans la séquence vidéo, la nouvelle position envoyée au serveur est postérieure à la position « attendue » par le serveur, c'est-à-dire la position correspondant à la dernière partie de l'information complémentaire envoyée par le serveur au client. L'envoi suivant du serveur est donc une partie de l'information complémentaire située après la dernière partie envoyée. La quantité de l'information complémentaire envoyée par le serveur dépend de la vitesse « avance rapide » qui a été choisie par le client. Cette fonctionnalité permet d'offrir plusieurs vitesses « avance rapide » sur l'équipement du client.

Pour améliorer la synchronisation entre le serveur et le client, l'invention comprend également un mécanisme d'accusation de réception. La portion d'information complémentaire envoyée par le serveur (12) est stockée dans le tampon d'entrée (86). Si le dispositif de synthèse (87) a besoin de cette information complémentaire pour reconstituer le flux originel et qu'il y arrive, le client (8) envoie un message de confirmation pour spécifier au serveur (12) s'il a bien reçu l'information complémentaire et s'il a été en mesure de l'utiliser pour l'affichage. Si le client n'a pas pu utiliser l'information complémentaire, cela signifie pour le serveur que celle-ci est arrivée trop tard (après le moment où elle devait être utilisée) et donc que le client et le serveur sont désynchronisés. Dans ce cas, le tampon d'entrée (86) est vide et le serveur (12) adapte le flux d'informations qu'il envoie pour faire en sorte de remplir

ce tampon. Pour cela, le serveur (12) doit anticiper plus longuement la lecture du client (8). Il dispose alors de deux solutions :

- soit il augmente le nombre d'images dans le prochain paquet. Cette solution permet de conserver la continuité du flux affiché, mais nécessite un réseau (10) de taille suffisante pour supporter une augmentation momentanée du trafic ;

- soit il choisit une portion d'information complémentaire postérieure à celle qu'il devrait envoyer pour assurer la continuité du flux vidéo. Alors, les images pour lesquelles aucune information complémentaire n'est envoyée restent embrouillées.

Dans un autre exemple de réalisation, le protocole réseau utilisé pour les communications entre le client et le serveur est UDP (« User Datagram Protocol »).

Enfin, un autre mode de mise en œuvre est décrit par la suite, concernant la synchronisation dans un système de protection appliqué à des flux audiovisuels au format MPEG-2 TS (« Transport Stream » en anglais, ou flux pour le transport), défini par la norme MPEG-2 pour une diffusion de données robuste aux erreurs de transmission sur les réseaux. Chacune des pistes audio ou vidéo contenues dans le flux est décomposée en une série de paquets de 188 octets, appelés paquets TS. Chaque paquet TS contient une entête indiquant à quelle piste audio ou vidéo le paquet est rattaché, l'ordre de traitement des paquets et les informations de synchronisation des pistes audio et vidéo associées.

Lors de l'étape d'embrouillage, certains des paquets TS relatifs aux flux vidéos sont substitués par des paquets « leurres » conformes à la norme, dans le but de dégrader visuellement le flux vidéo. Chaque paquet MPEG-2 TS au sein

du flux est identifié de manière unique, afin de synchroniser correctement le flux principal modifié et l'information complémentaire, et de réinsérer les paquets d'origine dans le flux lors de la phase de désembrouillage.

L'opération de désembrouillage du flux protégé par substitution de paquets TS est simple et efficace. Le module de désembrouillage utilise des informations relatives à l'encapsulation MPEG-2 TS des données, appelées « identifiants », sans utiliser les données relatives au contenu vidéo pour la synchronisation.

Lesdits identifiants utilisés pour la synchronisation sont :

- le PID (« Program Identity » en anglais) ou « identifiant de programme » du paquet substitué ;
- le « continuity counter » en anglais ou « compteur de continuité » du paquet substitué;
- la dernière PCR (« Program Clock Reference » en anglais) ou «horloge de référence» rencontrée, relative au flux vidéo concerné;
- l'index d'occurrence dudit compteur de continuité depuis le dernier paquet MPEG-2 TS renfermant un PCR. Cet index n'étant pas présent dans l'entête des paquets TS, est calculé lors des phases d'embrouillage et de désembrouillage.

L' « identifiant de programme » d'un paquet TS est situé dans l'entête de chaque paquet TS permettant à un décodeur MPEG-2 d'associer tous les paquets TS relatifs à un même flux lors du démultiplexage.

Le « compteur de continuité » d'un paquet TS est un compteur cyclique variant entre 0 et N-1 et permet de remettre les paquets en ordre en cas de permutation ou de

perte de paquets, dus à une erreur de transmission réseau, dans un groupe de N paquets consécutifs.

L' «horloge de référence» est un champ binaire optionnel et sert au décodeur pour calculer une base de temps.

L'index d'occurrence du compteur de continuité non présent dans les paquets TS, est calculé par le module d'analyse et d'embrouillage (12). Ledit index d'occurrence correspond, pour un paquet donné, au nombre de paquets TS ayant la même horloge de référence et le même compteur de continuité, qui se sont succédés depuis le dernier champ d'horloge de référence. L'horloge de référence est relative à l'identifiant de programme du paquet. En conséquence, un paquet TS contenant une horloge de référence, aura nécessairement un index d'occurrence de 1. Le paquet TS de même identifiant de programme et de même compteur de continuité qui suivra aura donc un index d'occurrence de 2 (si aucune horloge de référence ne s'est glissée pour ce flux entre temps). Les index d'occurrence des paquets suivants sont incrémentés de 1 si leur compteur de continuité a tourné d'un cycle (N) et leur identifiant de programme est identique, et ce, jusqu'à ce qu'une nouvelle horloge de référence relative au même flux soit rencontrée.

Lorsque le module d'embrouillage sauvegarde dans l'information complémentaire les paquets TS d'origine qui ont été substitués, il leur associe systématiquement les quatre identifiants cités précédemment:

- L'identifiant de programme du paquet permet, côté client, de savoir à quel flux élémentaire appartient le paquet.
- La dernière horloge de référence rencontrée permet de situer la tranche temporelle (avec une

granularité de 100 ms) à laquelle appartient le paquet.

° L'index d'occurrence du compteur de continuité permet d'identifier un groupe de N paquets TS auquel appartient le paquet.

° Le compteur de continuité permet d'identifier à quel paquet exactement on fait référence au sein de ce groupe de N paquets.

Ces quatre identifiants sont utilisés pour la synchronisation lors de la phase de désembrouillage, l'index d'occurrence du compteur de continuité étant également recalculé lors de la phase de désembrouillage.

Par exemple, dans une solution de diffusion de flux MPEG-2 TS protégés en temps réel, lorsque le client (8) souhaite visualiser le flux, le serveur envoie au préalable une partie de l'information complémentaire contenant des paquets TS d'origine, incluant des informations de synchronisation TS associés. Lorsque le module de désembrouillage (87) reçoit un paquet d'information complémentaire, il réalise à l'aide des identifiants de synchronisation la correspondance avec les paquets du flux principal modifié et les substitue par les paquets originaux présents dans l'information complémentaire.

Dans le cadre d'une application de vidéo à la demande, le module de désembrouillage transmet régulièrement au serveur (12) les identifiants de synchronisation issus des paquets du flux principal modifié qui est en cours de désembrouillage et d'affichage sur l'écran de visualisation (6). De cette manière, le serveur (12) en déduit la portion d'information complémentaire dont le client aura besoin dans les instants à venir et lui envoie les paquets nécessaires de l'information complémentaire.

REVENDICATIONS

1. Procédé pour la distribution de séquences vidéos selon un format de flux nominal constitués par une succession d'images, ledit flux sur lequel on procède, avant la transmission à l'équipement client, à une analyse pour générer un flux principal modifié, présentant le format du flux nominal, et présentant des images modifiées par la substitution de certaines données par des données de même nature mais aléatoires ou calculées, et une information complémentaire d'un format quelconque, comportant les données substituées et les informations numériques aptes à permettre la reconstruction dudit flux nominal modifié, puis à transmettre séparément, le flux principal modifié en temps réel ou en temps différé et l'information complémentaire en temps réel au moment de la visualisation depuis le serveur vers l'équipement destinataire, et pour lequel on calcule sur l'équipement destinataire une synthèse d'un flux disponible au format nominal, reconstitué en fonction dudit flux principal modifié et de ladite information complémentaire et une lecture dudit flux disponible sur l'équipement destinataire caractérisé en ce que ledit procédé comporte, pendant ladite lecture dudit flux, une étape consistant à générer un identifiant de position en fonction d'une caractéristique dudit flux lu, cet identifiant de position étant transmis au serveur activant en réponse l'envoi de l'information complémentaire en fonction dudit identifiant de position.

2. Procédé pour la distribution de séquences vidéos selon la revendication 1, caractérisé en ce que chaque image du flux nominal est associée à un indicateur de position.

3. Procédé pour la distribution de séquences vidéos selon la revendication 1, caractérisé en ce que l'étape de

lecture comporte une opération de calcul de l'identifiant de position de l'image lue.

4. Procédé pour la distribution de séquences vidéos selon la revendication 1, caractérisé en ce que l'étape de lecture comporte une opération de calcul de l'identifiant de position du flux lu.

5. Procédé pour la distribution de séquences vidéos selon la revendication 1, caractérisé en ce que l'information complémentaire est envoyée par portions.

6. Procédé pour la distribution de séquences vidéo selon la revendication 1, caractérisé en ce que le flux disponible sur l'équipement destinataire dont la lecture conditionne la position et la portion à envoyer de ladite information complémentaire est une partie du flux principal modifié.

7. Procédé pour la distribution de séquences vidéo selon la revendication 1, caractérisé en ce que le flux disponible sur l'équipement destinataire dont la lecture conditionne la position et la portion à envoyer de ladite information complémentaire est une partie du flux nominal reconstitué.

8. Procédé pour la distribution de séquences vidéo selon l'une des revendications précédentes, caractérisé en ce que le format de flux nominal est défini par la norme MPEG-2.

9. Procédé pour la distribution de séquences vidéo selon la revendication 8, caractérisé en ce que ledit identifiant de position pour une image est constitué des variables code temporel du groupe d'images dans lequel se trouve ladite image et référence temporelle de ladite image.

10. Procédé pour la distribution de séquences vidéo selon l'une des revendications précédentes, caractérisé en ce que le format de flux nominal est au format MPEG-2 TS et que ledit identifiant de position est constitué des quatre variables identifiant de programme, horloge de référence, compteur de continuité et index d'occurrence du compteur de continuité, ledit index d'occurrence du compteur de continuité résultant d'un calcul appliqué sur les paquets TS.

11. Procédé pour la distribution de séquences vidéo selon l'une des revendications précédentes, caractérisé en ce que chaque portion de ladite information complémentaire envoyée par le serveur permet de reconstituer au moins une image du flux originel lors de ladite synthèse.

12. Procédé pour la distribution de séquences vidéo selon l'une des revendications précédentes, caractérisé en ce que le serveur adapte la taille et le contenu de chaque portion de ladite information complémentaire à envoyer en fonction dudit identifiant de position.

13. Procédé pour la distribution de séquences vidéo selon l'une des revendications précédentes, caractérisé en ce que chaque portion de ladite information complémentaire est envoyée en avance par rapport à l'instant d'affichage de ladite image du flux reconstituée avec ladite portion.

14. Procédé pour la distribution de séquences vidéo selon l'une des revendications précédentes, caractérisé en ce que le serveur adapte l'envoi d'information complémentaire, lorsque l'utilisateur de l'équipement destinataire fait « pause », en arrêtant l'envoi de l'information complémentaire.

15. Procédé pour la distribution de séquences vidéo selon l'une des revendications précédentes, caractérisé en ce que le serveur adapte l'envoi d'information

complémentaire, lorsque l'utilisateur de l'équipement destinataire fait « avance rapide » ou « retour rapide », en envoyant la portion correspondant à la position adéquate pour les commandes « avance rapide » et « retour rapide ».

16. Procédé pour la distribution de séquences vidéo selon l'une des revendications précédentes, caractérisé en ce que le serveur adapte l'envoi d'information complémentaire, lorsqu'une panne réseau survient qui empêche la communication client – serveur, en arrêtant l'envoi d'information complémentaire durant la panne et le reprenant lorsque la panne cesse et qu'il reçoit de nouveau les messages en provenance du client.

17. Procédé pour la distribution de séquences vidéo selon l'une des revendications précédentes, caractérisé en ce que le serveur crée, préalablement à l'envoi de l'information complémentaire, un tableau associant des pointeurs vers des portions de l'information complémentaire avec des positions temporelles relatives à des images du flux vidéo, stocke ledit tableau sur un support relié au serveur et consulte ledit tableau pour déterminer la portion d'information complémentaire à envoyer après avoir reçu ledit identifiant de position.

18. Equipement pour la fabrication d'un flux vidéo en vue de la mise en œuvre du procédé selon l'une des revendications précédentes, comportant au moins un serveur multimédia contenant les séquences vidéos originelles, un dispositif d'analyse du flux vidéo provenant dudit serveur pour générer ledit flux principal modifié et ladite information complémentaire caractérisé en ce qu'il comprend un dispositif de synchronisation de l'envoi de ladite information complémentaire en fonction dudit identifiant de position envoyé par l'équipement destinataire.

19. Système pour la transmission d'un flux vidéo selon les revendications 1 à 16, caractérisé en ce qu'il comprend un équipement de production d'un flux vidéo, au moins un équipement d'exploitation d'un flux vidéo et au moins un réseau de communication entre l'équipement de production et le(s)équipement(s)d'exploitation.

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/FR 03/50158

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04N7/173 H04N7/167

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04N

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y	WO 00/44172 A (INTEL CORP ;RAMAKESAVAN SUNDARAM (US)) 27 juillet 2000 (2000-07-27) abrégé page 1, ligne 22 - ligne 26 page 2, ligne 14 - ligne 26 page 4, ligne 7 - ligne 10 page 4, ligne 16 - ligne 23 revendications 1,4,5,10-14 figures 1,2 ----- -/--	1-5,8,9, 11-14, 18,19

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe *ou la théorie constituant la base de l'invention*

"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du *présent* rapport de recherche internationale
18 mai 2004	11/06/2004

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Beaudet, J-P

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y	US 2002/164024 A1 (HATA KOICHI ET AL) 7 novembre 2002 (2002-11-07) abrégé alinéas '0009! - '0012!, '0039! - '0044!, '0051!, '0061! revendications 1,4-6,12,15 figures 1,9,10	1-5,8,9, 11-14, 18,19
A	WO 02/15579 A (GEN INSTRUMENT CORP ;SO NICOL CHUNG PANG (US)) 21 février 2002 (2002-02-21) abrégé page 2, ligne 16 - page 3, ligne 2 page 4, ligne 6 - ligne 15 page 5, ligne 3 - page 6, ligne 22 page 11, ligne 14 - page 13, ligne 11 page 14, ligne 8 - page 15, ligne 12 revendications 1,5-7,9,11,17,21,22,25,28,29 figures 2,3	1,2,4,5, 8,13-15, 17-19
A	WO 01/78386 A (WAJS ANDREW AUGUSTINE ;IRDETO ACCESS BV (NL)) 18 octobre 2001 (2001-10-18) abrégé page 1, ligne 26 - ligne 29 page 2, ligne 19 - ligne 33 page 4, ligne 7 - ligne 13 page 5, ligne 16 - ligne 36 page 7, ligne 10 - ligne 36 revendications 1,2,6-14 figure 1	1,2,4,8, 12,15, 17-19
A	EP 0 949 815 A (NIPPON ELECTRIC CO) 13 octobre 1999 (1999-10-13) abrégé alinéas '0008!, '0012!, '0014!, '0016!, '0017!, '0022! - '0029!, '0041! revendications 1,3,5,7,8,10 figure 2	1,5,8, 12,18,19
A	FR 2 812 147 A (INNOVATRON SA) 25 janvier 2002 (2002-01-25) abrégé page 3, ligne 10 - ligne 21 page 3, ligne 28 - page 4, ligne 12 page 6, ligne 34 - page 7, ligne 5 page 9, ligne 2 - ligne 20 revendications 1,4 figures 1,2	1,5,18, 19

-/--

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale No
PCT/FR 03/50158

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
WO 0044172	A	27-07-2000	AT	237904 T	15-05-2003
			AU	752973 B2	03-10-2002
			AU	2410300 A	07-08-2000
			CA	2359975 A1	27-07-2000
			CN	1338180 T	27-02-2002
			DE	60002158 D1	22-05-2003
			DE	60002158 T2	04-03-2004
			EP	1145551 A1	17-10-2001
			JP	2002535931 T	22-10-2002
			RU	2219678 C2	20-12-2003
			WO	0044172 A1	27-07-2000
US 2002164024	A1	07-11-2002	AU	7673101 A	04-03-2002
			EP	1313318 A1	21-05-2003
			WO	0217637 A1	28-02-2002
			JP	2002204220 A	19-07-2002
WO 0215579	A	21-02-2002	WO	0215579 A1	21-02-2002
			AU	4814400 A	25-02-2002
			CA	2408232 A1	21-02-2002
			EP	1275250 A1	15-01-2003
WO 0178386	A	18-10-2001	AU	6211801 A	23-10-2001
			BR	0109857 A	15-07-2003
			CA	2405262 A1	18-10-2001
			CN	1422492 T	04-06-2003
			WO	0178386 A2	18-10-2001
			EP	1290877 A2	12-03-2003
			JP	2003530784 T	14-10-2003
			TW	515203 B	21-12-2002
			US	2003237089 A1	25-12-2003
EP 0949815	A	13-10-1999	JP	11298878 A	29-10-1999
			CA	2268762 A1	08-10-1999
			EP	0949815 A2	13-10-1999
			US	6584200 B1	24-06-2003
FR 2812147	A	25-01-2002	FR	2812147 A1	25-01-2002
US 2001036355	A1	01-11-2001	CN	1381056 T	20-11-2002
			WO	0175888 A1	11-10-2001
			EP	1275115 A1	15-01-2003
			HU	0201823 A2	28-09-2002
			JP	2003529991 T	07-10-2003

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	GRIWODZ C ET AL: "PROTECTING VOD THE EASIER WAY" PROCEEDINGS OF THE ACM MULTIMEDIA 98. MM '98. BRISTOL, SEPT. 12 - 16, 1998, ACM INTERNATIONAL MULTIMEDIA CONFERENCE, NEW YORK, NY : ACM, US, vol. CONF. 6, 12 septembre 1998 (1998-09-12), pages 21-28, XP000977484 ISBN: 1-58113-036-8 abrégé alinéa '04.1! figure 1	1,5,11, 13,18,19
A	JARMASZ J P ET AL: "Designing a distributed multimedia synchronization scheduler" MULTIMEDIA COMPUTING AND SYSTEMS '97. PROCEEDINGS., IEEE INTERNATIONAL CONFERENCE ON OTTAWA, ONT., CANADA 3-6 JUNE 1997, LOS ALAMITOS, CA, USA,IEEE COMPUT. SOC, US, 3 juin 1997 (1997-06-03), pages 451-457, XP010239219 ISBN: 0-8186-7819-4 abrégé alinéas '0003!, '04.2!	6,7,12, 13
A	US 2001/036355 A1 (MORRIS OCTAVIUS J ET AL) 1 novembre 2001 (2001-11-01) abrégé figure 1 alinéas '0008!, '0015!, '0021!, '0025! - '0027!, '0050!, '0060! - '0065!	10